

ON THE AVERAGE EXPONENT OF CM ELLIPTIC CURVES MODULO p

KIM, SUNGJIN

ABSTRACT. Let E be an elliptic curve defined over \mathbb{Q} and with complex multiplication by \mathcal{O}_K , the ring of integers in an imaginary quadratic field K . Given $A > 0$, we have

$$(1) \quad \sum_{p \leq x} e_p = c_E \text{Li}(x^2) + O_{A,E}(x^2/(\log x)^A).$$

where

$$c_E = \sum_{k=1}^{\infty} \frac{1}{n_k} \sum_{dm=k} \frac{\mu(d)}{m},$$

and $n_k = [\mathbb{Q}(E[k]) : \mathbb{Q}]$. This improves the error term $x^2/(\log x)^{15/14}$ given by the recent work of Jie Wu [JW].

1. INTRODUCTION

Let E be an elliptic curve over \mathbb{Q} , and p be a prime of good reduction. Denote $E(\mathbb{F}_p)$ the group of \mathbb{F}_p -rational points of E . It is known that $E(\mathbb{F}_p)$ has a structure

$$(2) \quad E(\mathbb{F}_p) \simeq \mathbb{Z}/d_p\mathbb{Z} \oplus \mathbb{Z}/e_p\mathbb{Z}.$$

with $d_p|e_p$. By Weil's bound, we have

$$(3) \quad |E(\mathbb{F}_p)| = p + 1 - a_p$$

with $|a_p| < 2\sqrt{p}$. We fix some notations before stating results. Let $E[k]$ be the k -torsion points of the group $E(\overline{\mathbb{Q}})$. Denote $\mathbb{Q}(E[k])$ the k -th division field, which is obtained by adjoining coordinates of $E[k]$. Denote n_k the field extension degree $[\mathbb{Q}(E[k]) : \mathbb{Q}]$. Recently, T.Freiberg and P.Kurlberg [TP] started investigating the average order of e_p . They obtained that there exists a constant $c_E \in (0, 1)$ such that

$$(4) \quad \sum_{p \leq x} e_p = c_E \text{Li}(x^2) + O(x^{19/10}(\log x)^{6/5})$$

under GRH, and

$$(5) \quad \sum_{p \leq x} e_p = c_E \text{Li}(x^2) + O(x^2 \log \log \log x / \log x \log \log x).$$

unconditionally when E has CM. More recently, J.Wu [JW] improved their error terms in both cases

$$(6) \quad \sum_{p \leq x} e_p = c_E \text{Li}(x^2) + O(x^{11/6}(\log x)^{1/3})$$

under GRH, and

$$(7) \quad \sum_{p \leq x} e_p = c_E \text{Li}(x^2) + O(x^2/(\log x)^{15/14}).$$

unconditionally when E has CM.

In this paper we improve the unconditional error term in CM case.

Theorem 1.1. *Let E be a CM elliptic curve defined over \mathbb{Q} and with complex multiplication by \mathcal{O}_K , the ring of integers in an imaginary quadratic field K . Given $A > 0$, we have*

$$(8) \quad \sum_{p \leq x} e_p = c_E \text{Li}(x^2) + O_{A,E}(x^2/(\log x)^A).$$

where

$$c_E = \sum_{k=1}^{\infty} \frac{1}{n_k} \sum_{dm=k} \frac{\mu(d)}{m}.$$

2. PRELIMINARIES

Lemma 2.1. *Let E be a CM elliptic curve defined over \mathbb{Q} and with complex multiplication by \mathcal{O}_K . Then for $k > 2$,*

$$\phi(k)^2 \ll n_k \ll k^2$$

where ϕ is the Euler function.

Lemma 2.2. *Let E be an elliptic curve over \mathbb{Q} , and p be a prime of good reduction. Then*

$$k|d_p \Leftrightarrow p \text{ splits completely in } \mathbb{Q}(E[k]).$$

Proof. See [M], p159. □

Let N be the conductor of E , and denote

$$\pi_E(x; k) = \#\{p \leq x : p \nmid N, \text{ } p \text{ splits completely in } \mathbb{Q}(E[k])\}$$

Lemma 2.3. *For $2 \leq k \leq 2\sqrt{x}$, we have*

$$\pi_E(x; k) \ll \frac{x}{k^2}$$

where the implied constant is absolute.

Proof. See A.Cojocaru [AC], Lemma 2.6, and note that there are only nine possibilities of K . □

We state some class field theory background. For the proofs, see [AM], Lemma 2.6, 2.7.

Lemma 2.4. *If $m \geq 3$ then $\mathbb{Q}(E[m]) = K(E[m])$.*

Lemma 2.5. *Let E/\mathbb{Q} have CM by \mathcal{O}_K and $m \geq 1$ be an integer. Then there is an ideal \mathfrak{f} of \mathcal{O}_K and $t(m)$ ideal classes mod $\mathfrak{f}m$ with the following property:*

If \mathfrak{p} is a prime ideal of \mathcal{O}_K with $\mathfrak{p} \nmid \mathfrak{f}m$, then

\mathfrak{p} splits completely in $K(E[m]) \Leftrightarrow \mathfrak{p} \sim \mathfrak{m}_1$, or \mathfrak{m}_2 , or \dots , or $\mathfrak{m}_{t(m)}$ mod $\mathfrak{f}m$.

Moreover

$$t(m)[K(E[m]) : K] = h(\mathfrak{f}m),$$

where

$$t(m) \leq c\phi(\mathfrak{f}) \prod_{\mathfrak{p}|\mathfrak{f}} \left(1 + \frac{1}{N(\mathfrak{p}) - 1}\right).$$

Here c is an absolute constant and $\phi(\mathfrak{f})$ is the number field analogue of the Euler function.

Let $\pi_K(x; \mathfrak{q}, \mathfrak{a}) = \#\{\mathfrak{p} : \text{prime ideal; } N(\mathfrak{p}) \leq x, \text{ and } \mathfrak{p} \sim \mathfrak{a} \bmod \mathfrak{q}\}$. The following is a number field analogue of the Bombieri-Vinogradov theorem due to Huxley [H], Theorem 1.

Lemma 2.6. *For each positive constant B , there is a positive constant $C = C(B)$ such that*

$$\sum_{N(\mathfrak{q}) \leq Q} \max_{(\mathfrak{a}, \mathfrak{q})=1} \max_{y \leq x} \frac{1}{T(\mathfrak{q})} \left| \pi_K(y; \mathfrak{q}, \mathfrak{a}) - \frac{Li(y)}{h(\mathfrak{q})} \right| \ll \frac{x}{(\log x)^B},$$

where $Q = x^{1/2}(\log x)^{-C}$. The implied constant depends only on B and on the field K .

We are now ready to prove Theorem 1.1. From now on, E is an elliptic curve over \mathbb{Q} that has CM by \mathcal{O}_K , where K is one of the nine imaginary quadratic field with class number 1. Let N be the conductor of E .

3. PROOF OF THE THEOREM 1.1

By Weil's bound, we have

$$(9) \quad \sum_{p \leq x, p \nmid N} e_p = \sum_{p \leq x, p \nmid N} \frac{p}{d_p} + O\left(\frac{x^{3/2}}{\log x}\right).$$

As shown in both [TP] and [JW], we use the following elementary identity

$$(10) \quad \frac{1}{k} = \sum_{dm|k} \frac{\mu(d)}{m}.$$

Thus we obtain

$$\begin{aligned} \sum_{p \leq x, p \nmid N} \frac{p}{d_p} &= \sum_{p \leq x, p \nmid N} p \sum_{dm|d_p} \frac{\mu(d)}{m} \\ &= \sum_{k \leq 2\sqrt{x}} \sum_{dm=k} \frac{\mu(d)}{m} \sum_{p \leq x, p \nmid N, k|d_p} p. \end{aligned}$$

Then we split the sum into two parts as in [JW].

$$\begin{aligned} S_1 &= \sum_{k \leq y} \sum_{dm=k} \frac{\mu(d)}{m} \sum_{p \leq x, p \nmid N, k|d_p} p, \\ S_2 &= \sum_{y < k \leq 2\sqrt{x}} \sum_{dm=k} \frac{\mu(d)}{m} \sum_{p \leq x, p \nmid N, k|d_p} p. \end{aligned}$$

Here $y \leq 2\sqrt{x}$ is to be chosen later. We treat S_2 using trivial estimate

$$(11) \quad \left| \sum_{dm=k} \frac{\mu(d)}{m} \right| \leq 1$$

and Lemma 2.3, then we obtain

$$(12) \quad |S_2| \ll \sum_{y < k \leq 2\sqrt{x}} x \cdot \frac{x}{k^2} \ll \frac{x^2}{y}.$$

Let $\pi_E(x; k) = \frac{\text{Li}(x)}{n_k} + E_k(x)$. Our goal for treating S_1 is making use of Lemma 2.6. First, we take care of the inner sum by partial summation

$$\begin{aligned} \sum_{p \leq x, p \nmid N, k|d_p} p &= \int_{2-}^x t d\pi_E(t; k) \\ &= x\pi_E(x; k) - \int_2^x \pi_E(t; k) dt \\ &= \frac{x\text{Li}(x)}{n_k} - \int_2^x \frac{\text{Li}(t)}{n_k} dt + O\left(x|E_k(x)| + \int_2^x |E_k(t)| dt\right) \\ &= \frac{1}{n_k} \text{Li}(x^2) + O\left(x \max_{t \leq x} |E_k(t)| + 1\right). \end{aligned}$$

Then we deal with S_1 using the trivial estimate (10) and Lemma 2.1, we have

$$(13) \quad S_1 = c_E \text{Li}(x^2) + O\left(x \max_{t \leq x} |E_2(t)|\right) + O\left(\frac{x^2}{y \log x} + \sum_{3 \leq k \leq y} x \max_{t \leq x} |E_k(t)| + \sqrt{x}\right)$$

where

$$c_E = \sum_{k=1}^{\infty} \frac{1}{n_k} \sum_{dm=k} \frac{\mu(d)}{m}.$$

Let $\widetilde{\pi}_E(x; k) = \#\{\mathfrak{p} : N(\mathfrak{p}) \leq x, \mathfrak{p} \nmid \mathfrak{f}\mathfrak{m}, \mathfrak{p} \text{ splits completely in } K(E[k])\}$. By Lemma 2.4, we have

$$(14) \quad \pi_E(x; k) = \frac{1}{2} \widetilde{\pi}_E(x; k) + O\left(\frac{x^{1/2}}{\log x}\right) \text{ uniformly for } k \geq 3.$$

For the detailed explanation, we refer to [AM], page 9. By Lemma 2.5, we have

$$(15) \quad \widetilde{\pi}_E(x; m) - \frac{\text{Li}(x)}{[K(E[m]) : K]} = \sum_{i=1}^{t(m)} \left(\pi_K(x, \mathfrak{f}\mathfrak{m}, \mathfrak{m}_i) - \frac{\text{Li}(x)}{h(\mathfrak{f}\mathfrak{m})} \right).$$

Again using Lemma 2.5 to bound $t(m)$ and applying Lemma 2.6,

$$(16) \quad \sum_{3 \leq k \leq x^{1/4}(\log x)^{-C}} \max_{t \leq x} \left| \widetilde{\pi}_E(t; k) - \frac{\text{Li}(t)}{[K(E[k]) : K]} \right| \ll \frac{x}{(\log x)^A}.$$

Note that $T(\mathfrak{q}) \leq 6$. Writing $\widetilde{E}_k(x) = \widetilde{\pi}_E(x; k) - \frac{\text{Li}(x)}{[K(E[k]) : K]}$, and using a bound for $\max_{t \leq x} |E_2(t)|$, we have

$$(17) \quad S_1 = c_E \text{Li}(x^2) + O\left(\frac{x^2}{(\log x)^A}\right) + O\left(\frac{x^2}{y \log x} + \sum_{3 \leq k \leq y} x \max_{t \leq x} |\widetilde{E}_k(t)| + \frac{x^{3/2}y}{\log x}\right)$$

Now, taking $y = x^{1/4}(\log x)^{-C}$, we obtain

$$(18) \quad S_1 = c_E \text{Li}(x^2) + O\left(x^{7/4}(\log x)^{C-1} + \frac{x^2}{(\log x)^A} + x^{7/4}(\log x)^{-1-C}\right).$$

Combining with estimate of $|S_2|$ in (11), it follows that

$$(19) \quad \sum_{p \leq x, p \nmid N} \frac{p}{d_p} = c_E \text{Li}(x^2) + O\left(\frac{x^2}{(\log x)^A} + x^{7/4}(\log x)^C\right).$$

Theorem 1.1 now follows.

REFERENCES

- [AC] A. Cojocaru, *Cyclicity of CM Elliptic Curves Modulo p* , Transaction of Americal Mathematical Society, volume 355, number 7
- [AM] A. Akbary, K. Murty, *Cyclicity of CM Elliptic Curves Mod p* , Indian Journal of Pure and Applied Mathematics, 41 (1) (2010), 25-37
- [H] M. Huxley, *The Large Sieve Inequality for Algebraic Number Fields III*, J. London Math. Soc. 3 (1971), 233-240
- [TP] T. Freiberg, P. Kurlberg, *On the Average Exponent of Elliptic Curves Modulo p* , www.math.kth.se/~tristanf/papers/freiberg-kurlberg-on-the-average-exponent-of-elliptic-curves-modulo-p.pdf
- [JW] J. Wu, *The Average Exponent of Ellptic Curves Modulo p* , arxiv.org/pdf/1206.5929v1.pdf
- [M] R. Murty, *On Artin's Conjecture*, Journal of Number Theory, Vol 16, no.2, April 1983